Unix Learning Journal

Penetration Testing

Trevor Kulczycki-McIntyre

Sunday April 28, 2024

In the first week of our project, we decided to keep things straightforward since none of us were too familiar with penetration testing. Our focus was on research and preparation. I took the responsibility of setting up Kali Linux and Parrot Security, ensuring they were ready for our upcoming tasks. Alongside this, I watched several YouTube videos to get acquainted with the Kali and Parrot environments. We obtained both Parrot Security and Kali Linux from osboxes.org, and we used VirtualBox as our hypervisor to boot the virtual machines. This laid a solid foundation for our project, allowing us to gradually delve into the complexities of penetration testing.

Wednesday May 8, 2024

This week I've made some additional progress in my learnings. I've been familiarizing myself with the Kali environment, as well as exploring my options in terms of which penetration testing software I will use. So far, I've tested out the Metasploit console, which was quite confusing to figure out. Networking is not an easy task for beginners. This week was another week of pure learning and playing around with Kali and nmap trying to wrap my head around a lot of new information in such a short period of time. In the coming days I plan to finalize my decision on which attack I'm going to perform and the software I plan to use to execute it. This has been an eye-opening experience for me since it shows I still have much more to learn, and that this is only the beginning.

Friday May 19, 2024

This week I have successfully hacked Metasploitable 2! I have attempted another time before this however it was to no avail since I was too unfamiliar with the software. Initially I thought the purpose was to hack into the Metasploit console. So I installed it and was trying to figure out how to hack into it for over 5 hours. Finally I had to take a step back

and think. I realized that the VM I was supposed to attack was Metasploitable 2, not the Metasploit console. In my defence I didn't know there was a difference. So this week I downloaded the correct VM and my hack was successful. I found this such an amazing and satisfying experience since hacking was always such a cool thing to me and I am glad I was able to take part in this. I used Nessus to scan vulnerabilities on the target VM network, and decided to perform an attack using the VNC server viewer (TigerVNC). This allowed me to remotely access the target's shell command terminal and run commands.

Kali Linux link: https://www.osboxes.org/kali-linux/

Metasploitable 2 link:
https://sourceforge.net/projects/metasploitable/files/latest/download

Nessus install link: https://www.tenable.com/downloads/nessus?loginAttempted=true

Parrot Security OS link: https://www.osboxes.org/parrot-security-os/

Useful Youtube Videos:
https://www.youtube.com/watch?v=8ucrQ6Tj2js&pp=ygUYaG93IHRvIHN0YXJ0IHBlbnRlc3Rpbmcg

https://www.youtube.com/watch?v=B7tTQ272OHE&pp=ygUYaG93IHRvIHN0YXJ0IHBlbnRlc3Rpbmcg

Github Link: https://github.com/Trevor-Km/Unix-Pen-Test-Final-Project